PROFESSIONAL-CLOUD-SECURITY-ENGINEER$^{Q\&As}$

Professional Cloud Security Engineer

Pass Google PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam with 100% Guarantee

QUESTION 1

You need to use Cloud External Key Manager to create an encryption key to encrypt specific BigQuery data at rest in Google Cloud. Which steps should you do first?

A. 1. Create or use an existing key with a unique uniform resource identifier (URI) in your Google Cloud project.

2. Grant your Google Cloud project access to a supported external key management partner system.

B. 1. Create or use an existing key with a unique uniform resource identifier (URI) in Cloud Key Management Service (Cloud KMS).

2. In Cloud KMS, grant your Google Cloud project access to use the key.

C. 1. Create or use an existing key with a unique uniform resource identifier (URI) in a supported external key management partner system.

2. In the external key management partner system, grant access for this key to use your Google Cloud project.

D. 1. Create an external key with a unique uniform resource identifier (URI) in Cloud Key Management Service (Cloud KMS).

2. In Cloud KMS, grant your Google Cloud project access to use the key.

Correct Answer: C

https://cloud.google.com/kms/docs/ekm#how_it_works

-First, you create or use an existing key in a supported external key management partner system. This key has a unique URI or key path.

-Next, you grant your Google Cloud project access to use the key, in the external key management partner system.

-In your Google Cloud project, you create a Cloud EKM key, using the URI or key path for the externally- managed key.

QUESTION 2

You are a Cloud Identity administrator for your organization. In your Google Cloud environment groups are used to manage user permissions. Each application team has a dedicated group Your team is responsible for creating these groups and the application teams can manage the team members on their own through the Google Cloud console. You must ensure that the application teams can only add users from within your organization to their groups.

What should you do?

A. Change the configuration of the relevant groups in the Google Workspace Admin console to prevent external users from being added to the group.

B. Set an Identity and Access Management (1AM) policy that includes a condition that restricts group membership to user principals that belong to your organization.

C. Define an Identity and Access Management (IAM) deny policy that denies the assignment of principals that are outside your organization to the groups in scope.

D. Export the Cloud Identity logs to BigQuery Configure an alert for external members added to groups Have the alert trigger a Cloud Function instance that removes the external members from the group.

Correct Answer: A

QUESTION 3

While migrating your organization\\'s infrastructure to GCP, a large number of users will need to access GCP Console. The Identity Management team already has a well-established way to manage your users and want to keep using your existing Active Directory or LDAP server along with the existing SSO password.

What should you do?

A. Manually synchronize the data in Google domain with your existing Active Directory or LDAP server.

B. Use Google Cloud Directory Sync to synchronize the data in Google domain with your existing Active Directory or LDAP server.

C. Users sign in directly to the GCP Console using the credentials from your on-premises Kerberos compliant identity provider.

D. Users sign in using OpenID (OIDC) compatible IdP, receive an authentication token, then use that token to log in to the GCP Console.

Correct Answer: B

https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-configuring-single-sign- on
https://cloud.google.com/blog/products/identity-security/using-your-existing-identity-management-system- with-google-cloud-platform

QUESTION 4

Your DevOps team uses Packer to build Compute Engine images by using this process:

1 Create an ephemeral Compute Engine VM.

2 Copy a binary from a Cloud Storage bucket to the VM\\'s file system.

3 Update the VM\\'s package manager.

4 Install external packages from the internet onto the VM.

Your security team just enabled the organizational policy. consrraints/compure.vnExtemallpAccess. to restrict the usage of public IP Addresses on VMs. In response your DevOps team updated their scripts to remove public IP addresses on

the Compute Engine VMs however the build pipeline is failing due to connectivity issues.

What should you do? Choose 2 answers

A. Provision a Cloud NAT instance in the same VPC and region as the Compute Engine VM

B. Provision an HTTP load balancer with the VM in an unmanaged instance group to allow inbound connections from the internet to your VM.

C. Update the VPC routes to allow traffic to and from the internet.

D. Provision a Cloud VPN tunnel in the same VPC and region as the Compute Engine VM.

E. Enable Private Google Access on the subnet that the Compute Engine VM is deployed within.

Correct Answer: AE

QUESTION 5

Your Google Cloud environment has one organization node, one folder named "Apps", and several projects within that folder. The organizational node enforces the constraints/ iam.allowedPolicyMemberDomains organization policy, which

allows members from the terramearth.com organization. The "Apps" folder enforces the constraints/iam.allowedPolicyMemberDomains organization policy, which allows members from the flowlogistic.com organization. It also has the

inheritFromParent:

false property.

You attempt to grant access to a project in the "Apps" folder to the user testuser@terramearth.com.

What is the result of your action and why?

A. The action succeeds because members from both organizations, terramearth.com or flowlogistic.com, are allowed on projects in the "Apps" folder.

B. The action succeeds and the new member is successfully added to the project\\'s Identity and Access Management (IAM) policy because all policies are inherited by underlying folders and projects.

C. The action fails because a constraints/iam.allowedPolicyMemberDomains organization policy must be defined on the current project to deactivate the constraint temporarily.

D. The action fails because a constraints/iam.allowedPolicyMemberDomains organization policy is in place and only members from the flowlogistic.com organization are allowed.

Correct Answer: D

The correct answer is D. The action fails because a constraints/iam.allowedPolicyMemberDomains organization policy is in place and only members from the flowlogistic.com organization are allowed.

The inheritFromParent: false property on the "Apps" folder means that it does not inherit the organization policy from the organization node. Therefore, only the policy set at the folder level applies, which allows only members from the flowlogistic.com organization. As a result, the attempt to grant access to the user testuser@terramearth.com fails because this user is not a member of the flowlogistic.com organization.

Latest PROFESSIONAL-CLOUD-SECURITY-ENGINEER Dumps

PROFESSIONAL-CLOUD-SECURITY-ENGINEER Practice Test

PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam Questions